United States v. Taylor Huddleston

EXHIBIT 4 (James O'Gorman Declaration)

UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Criminal No. 1:17-CR-34
v.	)	Hon. Liam O'Grady
	)	
TAYLOR HUDDLESTON,	)	
	)	
Defendant.	)	

DECLARATION OF JAMES O'GORMAN

I, James O'Gorman, pursuant to 28 U.S.C. § 1746, make the following declaration:

Introduction

1. I am President of Offensive Security Services, located in Cornelius, North Carolina (telephone: 402-608-137; email: jim@offensive-security.com). A copy of my resume is attached. I have been retained by the Office of the Federal Public Defender to provide an opinion on aspects of a letter from Symantec by Bill Wright dated January 5, 2018. I understand that a copy of that letter has been provided to the Probation Officer. My opinions are my own based on my years of experience and expertise. They do not necessarily reflect the opinions of any company, organization, or affiliation.

Qualifications

2. I am President of Offensive Security Services, a leading information security training and services company. I have been working in this field for 20 years. My areas of expertise include, but are not limited to Information Security Training, Vulnerability Analysis, Penetration Testing, Exploit Development, Cyber Attack Scenario Planning, PCI security, Computer Forensics, and Incident Response. I have served in both technical and leadership

positions, including IT Manager, Technology Manager, and IT Director. I have also been a founder for Social-Engineer.org, and an instructor and mentor in both ethical hacking and computer forensics. I am also author of the books "Metasploit: The Penetration Tester's Guide" (published in 2011) and "Kali Linux Revealed" (published in 2017).

The Symantec Letter Dated January 5, 2018 from Bill Wright

3. The letter from Symantec provided information on the detection of NanoCore during a three-year period from December 14, 2014 through December 13, 2017. The Letter states that "Symantec received notifications of [NanoCore] detections from 107,813 unique devices globally." The Letter defines a "detection" as meaning that "one of our security products installed on a device has identified the presence of a file that meets the technical specifications provided in a malware definition."

Detections vs. Infections

4. In my opinion, the Symantec Letter is of limited utility because it does not distinguish between "detections" and "infections." A "detection" merely indicates the *presence* of the code on the device, but it does not indicate that the device has been *infected* with the malware. An "infection" means that the system was actually running malicious code on the host device. In my experience, damage would be present only on an "infected" system. Without the actual infection rate or a generally accepted percentage of detections that are assumed to be infections, it cannot be known (at least from the Symantec Letter) how many of the "detections" actually resulted in damage to a device.

Detections vs. Re-Detections

5. Further, although the Symantec Letter states the number of detections, it does not explain whether that number excludes re-detections (i.e., multiple detections) on the same device.

For instance, after an initial detection occurs, a clean-up tool may be used to remove the malware from the system. This clean up may leave behind artifacts that still trigger a "detection" by the anti-virus product. Or there may be instances where a security researcher is studying the malware and the anti-virus product detects the presence of the malware, but no removal occurs in response to this detection as the presence is intentional. Nor does the Letter explain how it ruled out the very common possibility that antivirus software could be detecting NanoCore that has been neutralized previously. Thus, the 107,813 figure may not accurately represent the number of devices infected.

False Positives

6. The Symantec Letter also does not take into account possible false positives, even on devices that are "infected" by malware. For example, the Letter does not rule out the possibility that malware with features similar to NanoCore (but not the NanoCore code itself) could result in a positive "detection." Relatedly, Symantec's 107,813 figure could include different malware that, as is common in computer intrusion cases, repurposed the NanoCore code in a way that would spur false positives. This is especially relevant here because of the leaks (or "cracking") of the NanoCore code. Symantec's Letter does not provide any information on the particular "signature" that Symantec used for detecting NanoCore and whether that "signature" was from the original source code or from a leaked or cracked version authored by others. Without knowing how wide a net Symantec cast, it is not possible to rule out the possibility that the 107,813 figure includes some or many false positives.

7. More particularly, with respect to the NanoCore code, according to multiple news sources[1] there were multiple instances of the leaking (cracking) of the NanoCore source code in 2013, 2014 (multiple times) and 2015. There is an understanding that malware authors will often take existing source code, like NanoCore, and use it for inspiration for their own software, or directly modify / port the source code into new derivatives. For instance, the "EternalBlue" exploit code developed by the National Security Agency (NSA) was leaked online and was directly used in multiple malware tools, including "WannaCry" and the "Retefe Banking Trojan."[2] Often times, these derivatives can be detected as if they are the original software due to the nature of signature detection being used in antivirus tools.
8. Symantec's method for ensuring that the purported "detections" were of the original Trojan.Nancrat tools (and not derivatives created from the multiple source code leaks) is especially important here. That's because, as noted in a report published on the official Symantec Blog,[3] the detection rates of the Trojan.Nancrat (NanoCore) had a significant increase after these source code leaks:

---

[1] See, e.g., Ensilo, *NanoCore Rat: It's Not 100% Original* (Apr. 13, 2015), available at https://blog.ensilo.com/nanocore-rat-not-100-original (last visited Jan. 24, 2018); Symantec Official Blog, *NanoCore: Another RAT tries to make it out of the Gutter* (Mar. 23, 2015) available at https://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter (last visited Jan. 24, 2018).

[2] *See* Wikipedia, *EternalBlue*, available at https://en.wikipedia.org/wiki/EternalBlue (last visited Jan. 24, 2018); Wikipedia, *WannaCry*, available at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (last visited Jan. 24, 2018), and Proofpoint, *Retefe Banking Trojan*, available at https://www.proofpoint.com/us/threat-insight/post/retefe-banking-trojan-leverages-eternalblue-exploit-swiss-campaigns (last visited Jan. 24, 2018).

[3] See Symantec Official Blog, *NanoCore: Another RAT tries to make it out of the Gutter* (Mar. 23, 2015) available at https://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter (last visited Jan. 24, 2018).

> The first cracked version of NanoCore was leaked in December 2013; but this was an alpha version with very few capabilities enabled. The second leak in mid-February 2014 was a beta version with many more capabilities enabled and it was shortly after this version was posted to underground forums that we began to see spikes in NanoCore detections. There was a relatively short period of time between the leak of the first beta version (1.0.2.0) and the first spike, possibly due to it taking time for the news to spread or the bad guys becoming familiar with the new RAT before they started using it.

Based on the numbers reported in the Symantec Letter, the vast majority of the detections occurred in 2017 well after multiple versions of the "Trojan.Nancrat" (NanoCore) leaked online.

I declare under penalty of perjury that the foregoing is true and correct. Executed on February 5th, 2018.

James O'Gorman